December 8, 2011

How to Craft Computer Policies on Personal Emails and Surfing

You have an unproductive employee. You suspect she isn't getting her work done because she's spending far too much time surfing the web and sending personal emails from her work computer during office hours. This will not do.

So, you log on to her computer after hours to check her inbox and browser history. Sure enough, your suspicions are correct: she's spending more time on Facebook than doing her job. Armed with this evidence, you call her into your office and dismiss her.

Problem solved? In fact, you might put your fi rm on the wrong side of an expensive lawsuit if you surreptitiously scrutinize an employee's computer usage and personal emails sent from a company account. A court could disqualify your carefully gathered evidence in an employee discipline or dismissal case *and* fine your firm thousands of dollars for breaching privacy.

It might come as a surprise that you don't have the right to view any data you wish on the computers you own. After all, the ownership of a given piece of property has historically been the main consideration in determining whether there is a reasonable expectation of privacy. Surely, an employee using a company computer has no expectation of privacy for information stored on it?

Yet, several recent court cases show that employees *do* have privacy rights in this area. And the principles in these cases apply to employers across Canada.

Last March, a case in the Ontario Court of Appeal tested employees' rights to data privacy. In *R. v. Cole*, the court held that a teacher had no reasonable expectation of privacy for a child-pornography image that a technician had discovered on the teacher's laptop during routine maintenance—because the employee knew the technician had access to the laptop for this purpose.

But the court also held that the police had violated the *Canadian Charter of Rights and Freedoms* by further searching the laptop's hard drive without a warrant. The court reached the latter conclusion because the school board had no clear policy permitting monitoring or searching of employees' computers; employees had exclusive possession of laptops for personal purposes and could take them home on evenings, on weekends and over the summer holidays; and the board allowed employees to store personal information on the laptops.

The court's discussion in this case of "a reasonable expectation of privacy" is part of a broader trend by courts, tribunals and labour arbitrators toward recognizing employee privacy rights for information stored on work computers.

Last May, a Quebec labour arbitrator ordered Laval University to pay punitive damages for violating an employee's privacy rights when she was using a university owned computer. Laval had conducted surveillance of emails between the employee and her union rep in an attempt to identify an information leak to the union. The university had a privacy policy allowing it to review employee emails if it suspected a policy or bylaw violation, needed information when the employee wasn't available or wanted to help a police investigation. But the arbitrator concluded that none of these circumstances applied in this case.

These cases reinforce the view that federal privacy commissioner Jennifer Stoddart stated in 2009 that "even where emails are sent or received by employees on an organization's system and are considered to be corporate records, such emails are also the employees' personal information." She concluded that an employer can review personal emails only if there is "a justifiable reason" to do so—even if the employer's policy specifies that messages saved on its computers are the employer's property.

Given these trends, the best way to protect your company from being found in violation of employee privacy is to adopt a well-conceived policy on computer usage and enforce it consistently. Here's what that policy should include:

- Explain that work computers and other electronic devices, including any information sent from or stored on them, are the employer's property, and that employees shouldn't assume the company has no right to search through this information

- Specify which technology the policy applies to—e.g., desktop computers, laptops, smartphones and other devices the firm issues for work-related purposes.

- Set limitations on personal use, including prohibitions on unlawful activity, use for inappropriate purposes and excessive personal use. You might want to forbid employee access to perceived time-sucking websites such as Facebook and personal email accounts such as Hotmail.

But you might be happy to have your people visit business-networking sites such as LinkedIn and social-media sites such as Twitter for business purposes. As well, consider limiting personal Internet usage to your employees' breaks. The key is to think carefully about the prohibited uses; Laval University ran into trouble because it failed to anticipate the case that landed it in court.

- Reserve your right to monitor employee usage and access personal information on company devices. You should set out the circumstances in which you would take such action, such as ensuring compliance with the law (e.g., viewing or storing child

pornography, or breaching copyright law by illegally downloading software, music or movies); investigating breaches of confidentiality and inappropriate disclosure of company information; ensuring a workplace free of harassment and discrimination; and accessing key information if the employee is unavailable. But don't make this list too exhaustive; for instance, the courts are likely to consider a policy permitting you to review all personal emails as too broad.

- Warn employees that a breach of the policy will result in discipline, up to and including dismissal for cause.

Once you've drafted a policy, review it annually to see whether all of it still make sense. For instance, you might wish to remove a no-Facebook provision if everyone, including management, is happily posting status updates.

What if you've adopted a policy, briefed employees and suspect that someone is still breaking the rules? Resist the impulse to snoop. Generally, you should raise the issue with the employee and advise him that you might start monitoring his Internet and email usage. But some cases, such as investigating workplace harassment, justify not alerting the employee before you review personal information on his work computer.

Although employee data privacy can be tricky to navigate, a clear and consistently applied computer-usage policy is your best line of defence against huge legal fees and a compromised reputation.

This article was published in the December 8, 2011 issue of Small Business Profit Guide.It can be read online at:http://www.profitguide.com/article/60922--how-to-craft-computer-policies-on-personal-emails-and-surfing

For more information please contact **Nicole Skuggedal** at nskuggedal@lawsonlundell.com or 604.631.6795.